

The Volokh Conspiracy | Opinion

Government ‘hacking’ and the Playpen search warrant

By **Orin Kerr** September 27

In recent months, over a dozen district courts have handed down divided opinions on the legality of a single search warrant that was used to search the computers of many visitors to a child pornography website. The warrant raises interesting legal issues, although I think the significant issues are mostly not the ones that have received the most media attention. Many of these cases are headed to various courts of appeal, so I thought I would present an overview of the investigation and discuss some of the legal issues raised by the warrant.

I. The Investigation

In September 2014, the federal government began investigating a child pornography website available only as a hidden service on the anonymized Tor network. The site, known as Playpen, could only be found if a person used Tor and knew the random string of numbers and letters that made up the site’s online address. In just a few months, Playpen drew more than 200,000 global users who contributed more than 100,000 posts. Every user had to log in with a username and password to visit the site. Thousands of posts on the site contained child pornography, and much of the rest of the site was discussions about child pornography.

As an anonymizing service, Tor hid the true IP addresses of Playpen account holders. Without knowing those IP addresses, there was no obvious way the government could identify and prosecute the account holders. The government devised the following strategy to reveal the users’ true location. After taking over the website pursuant to a warrant, the government obtained a second search warrant from a magistrate judge in the Eastern District of Virginia allowing the government to install a “network investigative technique” (“NIT”) on the computers of Playpen account holders. This second warrant is what I am calling the Playpen warrant.

According to the Playpen warrant, when a visitor logged in to the site with a username and password, the NIT would be secretly installed on the visitor’s personal computer. The NIT would then send the government identifying information about the user’s computer, most importantly the computer’s true IP address from inside the user’s machine.

For reasons I don’t quite understand, it appears that the government executed the warrant more narrowly than the warrant says. Although the warrant says that the NIT can be installed when a user logs in to his account, the government apparently

only installed the NIT when a logged-in user clicked on a link to access the ‘Preteen Videos—Girls Hardcore’ forum. But the warrant itself was written more broadly to authorize the use of the NIT when a user logged in to a Playpen account.

The big picture here is that the NIT was used to bypass the anonymizing feature of Tor. Tor hid the users’ IP addresses, but the NIT would go directly into the suspect’s computer and retrieve the real IP addresses that Tor had hidden. When investigators learned the targets’ actual IP address, and addresses resolved to addresses inside the United States, investigators could then get additional court orders to identify where in physical space the computer was likely located. They could then obtain additional search warrants to conduct searches there, searching homes for the computers and finding child pornography on the machines.

During the time that the NIT was used, as authorized by the warrant, it led to the installation of the NIT on more than 1,000 visitor computers. This led to around 200 nearly identical criminal cases all around the United States charging child pornography offenses. All of the charges stemmed from the one search warrant issued by a magistrate judge in the Eastern District of Virginia.

The Playpen case has received a lot of media attention, including about the ethics of the government running the Playpen server for a window of time while the monitoring occurred. For the rest of this post, I’ll pick just three among the many issues that have received attention or that I think deserve more attention.

II. Retrieving IP Addresses is Clearly a Search

A significant amount of media attention about the Playpen cases has focused on a curious argument. A minority of the judges have held that the the Playpen searches were constitutional because they weren’t searches at all. According to this argument, a person has no Fourth Amendment rights in IP addresses. Because the most important information obtained by the NIT was IP addresses, use of the NIT was not a search and no Fourth Amendment rights were violated. As far as I can tell, the government has not actually made this argument. Rather, it is a position introduced by one judge and then adopted by some others.

This argument is clearly wrong, though. Individuals have Fourth Amendment rights in information stored inside their computers unless they voluntarily share the information. A person using Tor has not voluntarily shared his IP address with the websites he visits. Indeed, the absence of voluntarily sharing is precisely what led the government to surreptitiously obtain the information using the NIT. Given that a Tor user has not voluntarily shared his IP address, it doesn’t matter that obtaining an IP address from a third party or a visited website would not be a search in other circumstances that did involve voluntarily sharing.

Put another way, it’s the way of obtaining information that makes the act a search, not the information itself in the abstract. This point is obvious in the physical world. *See Arizona v. Hicks*, 480 U.S. 321 , 325 (1987) (“A search is a search, even if it happens to disclose nothing but the bottom of a turntable.”). It should be equally obvious with computers. If the police want to read today’s newspaper, they can’t break into my house and open my desk drawer to find my copy without committing a search. The fact that they could have read the newspaper by finding a copy in public doesn’t mean they can break into my house to read

mine. Similarly, the fact that IP addresses may be available without searching a target in some cases doesn't mean they can break into his computer to find the IP address without committing a search.

III. Did the Warrant Particularly Describe the Place to be Searched?

A much more interesting question is whether the Playpen warrant satisfied the Fourth Amendment's requirement that warrants must particularly describe the place to be searched. Here's how the warrant described the place to be searched:

This warrant authorizes the use of a network investigative technique ("NIT") to be deployed on the computer server described below, obtaining information described in Attachment B from the activating computers below.

The computer server is the server operating the Tor network child pornography website referred to herein as the TARGET WEBSITE, as identified by its URL – [omitted]— which will be located at a government facility in the Eastern District of Virginia.

The activating computers are those of any user or administrator who logs into the TARGET WEBSITE by entering a username and password.

The place to be searched, in other words, was the "computers . . . of any user or administrator who logs into the TARGET WEBSITE by entering a username and password." Was this description constitutionally adequate?

I haven't seen good discussions of this in the cases so far. But it's a serious question, I think.

On one hand, courts have approved quite general descriptions of the place to be searched in cases that involved monitoring that would go to different and unknown places. For example, in *United States v. Karo*, 468 U.S. 705 (1984), the Supreme Court suggested that that warrants to install a locating beeper could simply name "the object into which the beeper is to be placed" as the place to be searched. Under this approach, the thing into which the surveillance tool is placed becomes the place to be searched for purposes of the warrant, even if the location where the surveillance will reveal the beeper to be is unknown and unknowable.

Lower courts have taken a similarly flexible approach in cases that involved roving wiretaps. *See, e.g., United States v. Petti*, 973 F.2d 1441, 1445 (9th Cir. 1992) (allowing roving wiretaps that name the place to be searched as any "telephone facilities actually used" by an identified speaker). Under that approach, it is at least plausible that listing the place to be searched as the "activating computers . . . of any user or administrator who logs into the TARGET WEBSITE by entering a username and password" satisfies the Fourth Amendment standard.

On the other hand, those precedents are potentially distinguishable because they involved the monitoring of a single suspect or single device. The Playpen warrant authorized searching an unlimited number of computers located all around the world. The place to be searched was not wherever a single suspect went, or a single item of property, but rather thousands of machines

located throughout the planet (or, if you assume that the warrant was only needed and effective inside national borders, hundreds of computers throughout the United States) in an automated process.

This raises an intriguing question: Is there a limit on how many different places can be searched under a single warrant while still satisfying the requirement that the warrant describe the “place to be searched”? Can a single warrant justify a search of thousands or even (hypothetically) millions of computers, all used by different people who don’t know each other? At what point does the use of a single warrant to search many places make the warrant a general warrant that the Fourth Amendment prohibits?

Resolution of these questions hinge in part on level of generality courts use to interpret the particularity-as-to-place requirement. Do you take it on its face, requiring a single place to be searched? Do you take it more generally as a concern with ensuring narrow warrants, so that the particularity requirement is met if the warrant is not too broad? Do you take it even more abstractly as reflecting a concern with avoiding searches of innocent people, so that the particularity requirement becomes part of the probable cause requirement?

For example, does the existence of probable cause as to each place (assumed for now) negate the particularity concern, or does the Fourth Amendment have a cap on the number of different places searched even if there is probable cause for each place? And if there is such a cap, is there a way to draft the warrant to allow such multiple automated searches? Or are such automated searches prohibited by the Fourth Amendment under the particularity requirement?

These are really interesting issues, I think, and the trial court decisions I have seen haven’t engaged much with them. I expect the appellate courts will hand down important rulings on these questions.

IV. Differing Standards for Suppression for Rule 41 Violations

A lot of the litigation on the Playpen warrant has focused on Federal Rule of Criminal Procedure 41(b), the venue provision for federal search warrants. The usual venue rule is that judges can only authorize searches of property in their district. The Playpen server was located in the Eastern District of Virginia, the same district where the warrant was obtained. But the user computers turned out to be located all over the world, leading to criminal charges all over the country. Defendants are now arguing that the evidence should be suppressed because the warrant violated the venue provision of Rule 41(b).

The Rule 41 issue is somewhat time-bound, as several judges have recognized. Rule 41(b) is set to change in December absent Congressional override. The new venue rule will allow judges in districts “where activities related to a crime may have occurred” to issue warrants “to use remote access to search electronic storage media and to seize or copy electronically stored information” outside their districts when the district where “the media or information is located has been concealed through technological means.” (For discussion of these amendments from me, see my participation on this panel from August starting at the 40-minute mark.)

Putting the merits of the Rule 41(b) question to the side, the Playpen litigation has exposed variations in the circuits on the suppression standard for Rule 41(b) violations. In some circuits, violations of Rule 41(b) can lead to suppression independently

of any Fourth Amendment violation if “the search might not have occurred or would not have been so abrasive if the Rule had been followed” or “there is evidence of intentional and deliberate disregard of a provision of the Rule.” *United States v. Krueger*, 809 F.3d 1109, 1114 (10th Cir. 2015).

Other circuits look to whether the search “offends concepts of fundamental fairness or due process.” *United States v. Hall*, 505 F.2d 961 (3d Cir. 1974). Some circuits have suggested that Rule 41(b) violations do not lead to suppression unless they are also constitutional violations, which in practice means that Rule 41(b) violations do not themselves lead to suppression. *See, e.g., United States v. Hornick*, 815 F.2d 1156, 1158 (7th Cir. 1987) (Easterbrook, J.) (“In light of *Leon*, it is difficult to anticipate any violation of Rule 41, short of a defect that also offends the Warrant Clause of the fourth amendment, that would call for suppression. Many remedies may be appropriate for deliberate violations of the rules, but freedom for the offender is not among them.”).

V. The Possibility of Supreme Court Review

One interesting aspect of the Playpen litigation is that any circuit splits on legal issues likely won’t be distinguishable on the facts. These cases are being brought all around the country, and they all stem from a single warrant. Challenges to the warrant involve the same facts, so disagreement on the law will likely lead to direct clashes among the circuits. It seems possible that the Supreme Court will end up resolving some of the issues raised by these warrants because the lower courts may end up dividing deeply in essentially the same case.

As I often say, stay tuned.

Orin Kerr is the Fred C. Stevenson Research Professor at The George Washington University Law School, where he has taught since 2001. He teaches and writes in the area of criminal procedure and computer crime law.